

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION**

PAYMENTECH, LLC and JPMORGAN §
CHASE BANK, N.A., §
§
Plaintiffs §
§
v. § Civil Action No. _____
§
LANDRY'S INC., as successor in interest to §
LANDRY'S MANAGEMENT, L.P., §
§
Defendant. §

PLAINTIFFS' ORIGINAL COMPLAINT

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiffs Paymentech, LLC (“Paymentech”) and JPMorgan Chase Bank, N.A. (“JPMC”) (collectively “Chase Paymentech”) file this Original Complaint against Defendant Landry’s Inc. (“Landry’s”), as successor in interest to Landry’s Management, L.P., and allege as follows:

I. PARTIES

1. Plaintiff JPMorgan Chase Bank, N.A. is a national banking association with its main office located in Columbus, Ohio. Accordingly, JPMorgan Chase Bank, N.A. is a citizen of Ohio.

2. Plaintiff Paymentech, LLC is a Delaware limited liability company. The sole member of Paymentech, LLC is JPMorgan Chase Bank, N.A. Accordingly, Paymentech, LLC is a citizen of Ohio.

3. Defendant Landry’s Inc. is a Delaware corporation with its principal place of business in Houston, Harris County, Texas. Accordingly, Landry’s Inc. is a citizen of Texas.

II. JURISDICTION AND VENUE

4. This Court has subject-matter jurisdiction over this case because complete diversity of citizenship exists between Plaintiffs, who are citizens of Ohio, and Defendant, who is a citizen of Texas, and because Plaintiffs seek damages in excess of \$75,000 exclusive of interest and costs. *See 28 U.S.C. §§ 1332, 1441(b).*

5. Venue is proper in the Houston Division of the Southern District of Texas because Landry's Inc.'s principal place of business is in Harris County, Texas. 28 U.S.C. § 1391(b)(1). Venue is also proper based on Section 15.10 of the parties' Select Merchant Payment Card Processing Agreement, executed on or about December 31, 2008, and amended on or about December 2015 (collectively the "Agreement"). The Agreement is attached hereto as Exhibit A and incorporated as if fully set out herein.

III. FACTS

6. This breach of contract case concerns Landry's refusal to indemnify Chase Paymentech after final assessments were imposed arising out of a significant data breach at numerous Landry's properties in several states from as early as May 2014 until December 2015. Despite the clear and unambiguous language of the contract between Landry's and Chase Paymentech, Landry's refuses to indemnify Chase Paymentech for these assessments, forcing Chase Paymentech to bring this lawsuit.

A. The Relationship Among the Parties

7. JPMC is a national banking association that has membership agreements with credit card companies, including Visa, Inc. and MasterCard Incorporated (hereinafter referred to collectively as "Payment Brands"). Paymentech is the payment processing and merchant acquiring business of JPMC. Through JPMC, Paymentech authorizes payment card transactions with

various merchants by virtue of Merchant Payment Card Processing Agreements.

8. Landry's is a merchant that operates several properties around the country, including restaurants, hotels and casinos. Landry's accepts Visa and MasterCard credit cards as a form of payment at its properties.

9. In a typical payment card transaction, the customer presents his or her credit card to the merchant. The merchant's point of sale system sends the information to a payment processor (here, Paymentech), which then obtains an authorization from the payment or card brand (*e.g.*, Visa, Inc. or MasterCard, Inc.) and the bank that issued the customer's card (the issuer or the issuing bank). The funds are ultimately collected and sent to the merchant's bank (the acquiring bank, *e.g.*, JPMC).

B. The Agreement

10. On or about December 31, 2008, JPMC, the acquiring bank; Paymentech, the payment processor; and Landry's, the merchant; entered into a Select Merchant Payment Card Processing Agreement (the "Agreement"). *See Ex. A.* Pursuant to the Agreement, Chase Paymentech agreed to provide payment card processing services to Landry's for transactions that were processed at Landry's properties. In return, Landry's agreed to compensate Chase Paymentech for these services for an initial term of five years.

11. Pursuant to the Agreement, Landry's agreed to abide by "all Payment Brand Rules," which includes the "bylaws, rules, and regulations, as they exist from time to time, of the Payment Brand Rules." Ex. A, Agreement, at §§ 1.3, 17. Included in the Payment Brand Rules, among other things, are Visa's Global Compromised Account Recovery ("GCAR") Program and MasterCard's Account Data Compromise ("ADC") Program. These programs are designed to address the needs of Payment Brand clients in the event of a large scale credit card data

compromise. In this regard, the Payment Brand Rules also require compliance with “Security Guidelines,” that incorporate the Payment Card Industry Data Security Standards. *Id.* §§ 12, 17.

12. In connection with Landry’s contractual obligation to comply with the Payment Brand Rules and Security Guidelines, Landry’s was also contractually obligated to indemnify Chase Paymentech for its failure to comply with the Payment Brand Rules that led to assessments, fines, or penalties by the Payment Brands. Indeed, as part of the bargained-for agreement, Landry’s expressly agreed to indemnify or reimburse Chase Paymentech for any “assessment, fine, or penalty imposed on [Paymentech] or [JPMC] and any related loss, cost or expense incurred by [Paymentech] or [JPMC]” assessed by the Payment Brands as a result of Landry’s **“failure to comply with the Payment Brand Rules, including the Security Guidelines, or the compromise of any Payment Instrument Information.”** Ex. A, Agreement, at § 12 (emphasis added).

13. Landry’s contractual obligation to indemnify Chase Paymentech for any assessments, fines or penalties was not conditioned upon any other events such as any determination that the assessments, fines, or penalties imposed by the Payment Brands were undisputed by Landry’s or subsequently determined by Landry’s to be legitimate. Instead, Landry’s obligation to indemnify Chase Paymentech for any assessments, fines or penalties was triggered when the Payment Brands imposed assessments on Chase Paymentech as a result of their investigations into the Data Breach. *Id.* § 17 (emphasis added). Pursuant to the Agreement, this provision in Section 12 survived the termination of the Agreement. *See id.* § 16.

14. On or about October 28, 2015, Landry’s provided Notice of Termination of the Agreement in compliance with Section 10.1.

C. The Data Breach

15. On or about December 2, 2015, Chase Paymentech discovered a credit card data compromise related to certain properties owned by Landry's (the "Data Breach").

16. An investigation confirmed that a significant Data Breach occurred at numerous Landry's properties in several states during the following periods: May 4, 2014 through March 15, 2015; May 5, 2015 through December 3, 2015; and March 16, 2015 through May 4, 2015. During the Data Breach, millions of credit card accounts were compromised at multiple Landry's properties across fourteen different merchant brands, such as Bubba Gump, McCormick & Schmick's, Rainforest Café, Saltgrass restaurants, among others (*i.e.*, Landry's Properties).

17. In sum, the investigation confirmed that Landry's allowed cardholder account data to be put at risk as a result of the Data Breach.

18. Landry's acknowledged the Data Breach in a December 17, 2015 press release where Landry's notified the public and its customers that it had received reports of unauthorized charges on certain payment cards and that it had begun an investigation into those reports. Landry's also stated that it was implementing enhanced payment system changes, both to the specific properties where the suspected activity occurred and the majority of its other properties, which would encrypt the credit card data throughout the processing system. Landry's admitted that, although the investigation was ongoing, it appeared the information affected in the Data Breach included the data contained in the magnetic strip on the back of payment cards, such as a cardholder's name, card number, expiration date, and internal verification code.

19. Indeed, following its investigation Landry's issued another press release on January 29, 2016, and confirmed that the Data Breach involved the installation of a program on payment processing devices at certain Landry's Properties. According to Landry's, the program was

designed to search for data from the magnetic stripe of payment cards that had been swiped (*i.e.*, cardholder name, card number, expiration date and internal verification code) as the data was being routed through affected systems. The Data Breach impacted a number of Landry's Properties such as restaurants, food and beverage outlets, spas, and entertainment destinations for several months from approximately May 2014 until December 2015.

20. In sum, the Data Breach involved the compromise of Payment Instrument Information as defined by the Agreement, including but not limited to, the cardholder's name, card number, expiration date, and internal verification code.¹ Ex. A, Agreement, at § 17.

21. Later in December 2015, following the discovery of the Data Breach, the parties entered into an amendment to the Select Merchant Payment Card Processing Agreement, which revoked the previous Notice of Termination with respect to "Existing Merchants" only.²

D. The Visa GCAR Program

22. As noted above, in connection with data breaches where credit card information is compromised, such as the one at issue here, Visa utilizes a Global Compromised Account Recovery ("GCAR") Program, which is designed to balance the needs of Visa clients in the event of a large scale card data compromise. The GCAR Program is designed to compensate issuing

¹ "Payment Instrument Information" is defined in the Agreement § 17 as:

[P]ersonal information related to a Customer or the Customer's Payment Instrument, that is obtained by [Landry's] from the Customer's Payment Instrument, or from the Customer in connection with his or her use of a Payment Instrument (for example a security code, a PIN number, or the customer's zip code when provided as part of an address verification system). Without limiting the foregoing, such information may include a **Customer's name, Payment Instrument account number and expiration date**, date of birth, PIN data, security code data such as CVV2, CVC2, and any data read, scanned, **or otherwise obtained from the Payment Instrument, whether printed thereon, or magnetically, electronically or otherwise stored thereon.**

² On December 6, 2016, Landry's provided written notice to Chase Paymentech that it was terminating the amendment to the Agreement effective June 4, 2017 for reasons unrelated to the Data Breach.

banks—banks that issue credit cards—for a portion of costs associated with counterfeit magnetic-stripe losses and/or PIN data fraud losses, as well as a portion of the associated operating expenses resulting from the compromise. These costs include, but are not limited to, card replacement, recoupment of disputed charges, legal fees, and an increase in labor due to customer inquiries related to the compromise. The GCAR Program is included in the Payment Brand Rules that Landry’s contractually agreed to abide by as part of its contract with Chase Paymentech.

23. Pursuant to the terms of the GCAR Program, following a card data compromise, Visa first determines if the compromise meets the GCAR Event Qualification Criteria. If so, Visa calculates the merchant acquirer’s liability (here, Chase Paymentech) pursuant to the rules of the GCAR program. Visa then notifies Chase Paymentech of the amount being assessed (“GCAR Assessment”) and qualification details. Chase Paymentech, on behalf of the merchant, then may exercise appeal rights by submitting any appeal documents within 30 days of the qualification summary. Finally, Chase Paymentech is debited the amount of the GCAR Assessment approximately 30 days after notification or the completion of the appeal process.

24. In accordance with the GCAR Program, Visa conducted an investigation and determined that the Data Breach qualified as a GCAR Event. Visa then calculated the total amount of liability for the Data Breach at \$12,678,367.13, and issued a Qualification Notification of GCAR Assessment on July 15, 2017, informing Chase Paymentech that the Data Breach events met all the criteria set forth by the GCAR rules, and were therefore eligible for assessment.

25. Upon receipt of the Qualification Notification of GCAR Assessment from Visa, on July 17, 2017, Chase Paymentech notified Landry’s of the GCAR Assessment, informed Landry’s of its appeal rights, and requested that Landry’s reimburse Paymentech for the full amount within 30 days as required by the Agreement.

26. On July 25, 2017, in direct contradiction to the terms of the Agreement, Landry's responded that it "disputes that it has any obligation to reimburse Paymentech, LLC ("Paymentech") for any amounts imposed and collected by Visa from JP Morgan Chase Bank ("Chase")." Landry's noted, however, that it believed Chase Paymentech had various grounds to appeal the GCAR Assessment and agreed to provide Chase Paymentech with information to use on its behalf in the appeal process.

27. Although the appeal of the GCAR Assessment is filed by the acquirer, the merchant (here, Landry's) provides the substantive arguments to support the appeal of the GCAR Assessment. Accordingly, Landry's provided Chase Paymentech with the substantive arguments to use in Chase Paymentech's appeal of the Visa GCAR Assessment with the understanding that Chase Paymentech would merely file the appeal on Landry's behalf.

28. On September 11, 2017, Chase Paymentech filed a GCAR Assessment appeal with Visa on behalf of Landry's, containing arguments, including among other things arguments challenging the validity of the assessments under the Payment Brand Rules and enclosing supporting documentation provided by counsel for Landry's.

29. On December 15, 2017, Visa responded to the GCAR Assessment appeal filed by Chase Paymentech on behalf of Landry's. Based on information and belief, Visa staff determined that credit card data was compromised and that Landry's failed to comply with multiple Payment Card Industry Data Security Standards in connection with the Data Breach, and recommended that the Visa Appeal Committee deny Landry's appeal.

30. Visa's Appeal Committee rejected Landry's arguments and denied Landry's appeal on January 31, 2018. The final amount assessed by Visa for Landry's Data Breach was \$12,678,367.13, which included the original assessment \$12,628,367.13 and an additional

\$50,000.00 fee for the costs associated with the appeal. That amount was debited from Chase Paymentech in March 2018.

31. The decision of Visa's Appeal Committee is final and terminates the GCAR process. The decision is not subject to further challenges or other appeal rights.

E. The MasterCard ADC Program

32. As noted above, MasterCard utilizes a program similar to Visa's GCAR Program called the Account Data Compromise ("ADC") Program. Like the Visa GCAR Program, the ADC Program is included in the Payment Brand Rules. Pursuant to the terms of the ADC Program, following a credit card data compromise, MasterCard first determines if the occurrence constitutes an ADC Event, which is defined as an occurrence that results, directly or indirectly, in the unauthorized access to or disclosure of MasterCard account data. If it does, MasterCard determines the total amount of acquirer liability, including the amount of Operational Reimbursement³ and/or Fraud Recovery.⁴ MasterCard then notifies the acquirer (here, Chase Paymentech) of the liability amount ("ADC Assessment") and qualification details. Chase Paymentech may then file an appeal within 30 days after receipt of the final notification. Finally, Chase Paymentech will be debited the amount of the ADC Assessment on the date specified in the final notification or in the appeal decision notification letter, if applicable. Landry's was contractually obligated to indemnify Chase Paymentech for the amount of liability assessed by MasterCard against Chase Paymentech.

33. In accordance with the ADC Program, MasterCard conducted an investigation and

³ The MasterCard Operational Reimbursement program enables an issuer to partially recover costs incurred in reissuing cards and for enhanced monitoring of compromised and/or potentially compromised MasterCard Accounts associated with an ADC Event.

⁴ The MasterCard Fraud Recovery program enables an issuer to recover partial counterfeit fraud losses associated with an ADC Event.

determined that the Data Breach qualified as an ADC Event. MasterCard then calculated the total amount of liability for Operational Reimbursement and Fraud Recovery at \$10,548,342.50, and issued a Notification of Account Data Compromise Event Responsibility and Final Acquirer Financial Responsibility Report on October 5, 2017.

34. Upon receipt of the Notification of Account Data Compromise Event Responsibility from MasterCard, on October, 5, 2017, Chase Paymentech sent Landry's the Final Acquirer Financial Responsibility Report, informed Landry's of its appeal rights, and requested that Landry's reimburse Chase Paymentech for the full amount of the ADC Assessment within 30 days as required under the Agreement.

35. On October 18, 2017, again in direct contradiction to the terms of the Agreement, Landry's responded that it "disputes that it has any obligation to indemnify JP Morgan Chase Bank, N.A. or Paymentech, LLC for the amount of any assessment MasterCard has elected to impose, whether under the Select Merchant Payment Card Processing Agreement between Landry's, Inc. as successor in interest to Landry's Management, L.P. and Paymentech, LLC for itself and on behalf of JP Morgan Chase Bank, N.A. (as amended, the "Agreement") or otherwise." Landry's noted, however, that it believed Chase Paymentech had various grounds to appeal the ADC Assessment and agreed to provide Chase Paymentech with information to use on its behalf in the appeal process.

36. Like an appeal of the GCAR Assessment, the appeal of the ADC Assessment is filed by the acquirer, but the merchant (here, Landry's) provides the substantive arguments to support the appeal of the ADC Assessment. Accordingly, Landry's provided Chase Paymentech with the substantive arguments to use in Chase Paymentech's appeal of the ADC Assessment with the understanding that Chase Paymentech would merely file the appeal on Landry's behalf.

37. On November 13, 2017, Chase Paymentech filed an ADC Assessment appeal on behalf of Landry's with MasterCard, containing arguments, including arguments challenging the validity of the assessments under Payment Brand Rules and enclosing supporting documentation provided by counsel for Landry's.

38. On February 21, 2018, MasterCard responded to the ADC Assessment appeal filed by Chase Paymentech on behalf of Landry's. Based on information and belief, MasterCard staff determined that Landry's failed to comply with multiple Payment Card Industry Data Security Standards in connection with the Data Breach, and that credit card data was compromised.

39. MasterCard considered the "totality of the circumstances" and "determined that a reduction of Chase's total financial responsibility for this Case in the amount of \$3,164,502.75 is appropriate," pursuant to its Security Rules. Thus, the total ADC Assessment that MasterCard determined in connection with the Data Breach was \$7,383,839.75. That amount was debited from Chase Paymentech in March 2018.

40. The decision of MasterCard is final and terminates the ADC appeal process. The decision is not subject to any further challenges or any other appeal rights.

F. Landry's Refusal to Reimburse Chase Paymentech

41. As noted above, Landry's had the opportunity to raise numerous arguments challenging the validity of the assessments in both the GCAR Assessment appeal to Visa and the ADC Assessment appeal to MasterCard. After considering these arguments, the Payment Brands rejected them and denied Landry's appeals. Under the GCAR and ADC rules, these decisions were final and not subject to further challenges or other appeal rights.

42. Accordingly, the Payment Brands determined that the total amount to be assessed as a result of the Data Breach that occurred at restaurants and entertainment facilities owned or

operated by Landry's is \$20,062,206.88: \$12,678,367.13 for the Visa GCAR Assessment and \$7,383,839.75 for the MasterCard ADC Assessment. Under the explicit and unambiguous terms of the Agreement, Landry's is contractually obligated to indemnify Chase Paymentech for this amount, whether Landry's agreed with the assessments or not. *See Ex. A, Agreement, at § 12.* Moreover, Landry's agreed to indemnify Chase Paymentech "from any losses, liabilities, and damages of any and every kind . . . arising out of any claim, complaint, or Chargeback . . . caused by [Landry's] noncompliance with this Agreement, the Operating Guide, or the Payment Brand Rules."

See id. § 11.2.

43. On March 23, 2018, Chase Paymentech sent Landry's a demand letter requesting that it indemnify Chase Paymentech for the \$20,062,206.88 assessed by Visa and MasterCard and debited from Chase Paymentech in connection with the Data Breach.

44. Despite its obligation under the Agreement, Landry's baldly refused to indemnify Chase Paymentech for the amounts assessed by the Payment Brands as a result of the Data Breach. Indeed, on April 23, 2018, Landry's informed Chase Paymentech that it did not have any obligation to indemnify Chase Paymentech for the GCAR or ADC Assessments.

45. Because Landry's refuses to comply with its contractual obligations pursuant to the Agreement, Chase Paymentech is forced to file this Complaint.

IV. CAUSES OF ACTION

Count I – Breach of Contract

46. Chase Paymentech repeats and re-alleges the foregoing allegations of Paragraphs 1 through 45 as if fully set forth herein.

47. The Agreement is a valid and enforceable agreement.

48. Chase Paymentech fully performed in accordance with the terms of the Agreement.

49. Pursuant to the Agreement, Landry's agreed to abide by the Payment Brand Rules, which include compliance with and participation in Visa's GCAR Program and MasterCard's ADC Program. Ex. A, Agreement, at § 1.3.

50. Also under the Agreement, Landry's was obligated to indemnify and reimburse Chase Paymentech for any assessments, fines, or penalties imposed on Chase Paymentech arising from the GCAR or ADC Programs. Ex. A, Agreement, at § 12; *see also id.* § 11.2.

51. This obligation to indemnify Chase Paymentech was not conditioned upon any determination that the assessments, fines, or penalties imposed by the Payment Brands were either undisputed or subsequently determined to be legitimate. Nor was this obligation to indemnify Chase Paymentech conditioned upon whether Landry's agreed with the assessments or not.

52. Visa and MasterCard determined that Landry's failed to comply with multiple Payment Card Industry Data Security Standards, and that Payment Instrument Information was compromised. Indeed, Landry's has admitted that Payment Instrument Information (*i.e.*, cardholder names, card numbers, expiration dates, and internal verification codes) was compromised as a result of the Data Breach that occurred between May 2014 and December 2015. Accordingly, under either contractual provision—failure to comply with the Payment Brand Rules **or** compromise of Payment Instrument Information—Landry's was obligated to indemnify and reimburse Chase Paymentech for any assessments, fines and penalties imposed on Chase Paymentech by the Payment Brands as a result of the Data Breach. *See* Ex. A, Agreement, at § 12.

53. Likewise, Landry's failure to comply with the Payment Card Industry Data Security Standards and, thus, the Payment Brand Rules, triggered Landry's obligation to indemnify Chase Paymentech for all “losses, liabilities, and damages of any and every kind,” including the GCAR and ADC Assessments, “arising out of any claim, complaint, or Chargeback.” *Id.* § 11.2.

54. Landry's breached the Agreement by failing to pay Chase Paymentech the \$20,062,206.88 assessed by the Payment Brands as a result of their investigations into the Data Breach.

55. All notices and demands required by law or contract have been given or are given in this Complaint.

56. As a result of this breach, Chase Paymentech has suffered damages in an amount in excess of the minimum jurisdictional limits of this Court. Chase Paymentech seeks its actual damages from Landry's including, but not limited to, the \$20,062,206.88 assessed and debited by the Payment Brands as a result of their investigations into the Data Breach, as well as any interest and costs allowed under law.

57. Chase Paymentech also seeks its attorney's fees under Texas Civil Practice & Remedies Code § 38.001(8) and Sections 11 and 12 of the Agreement. This action is founded on written contract, and Chase Paymentech is therefore entitled to recover its reasonable attorney's fees incurred in addition to the amounts otherwise recoverable. Chase Paymentech is represented by attorneys, and its claim was presented to Landry's more than thirty days prior to the trial of this action, and the just amount has not been tendered.

Count II (In the Alternative) – Quantum Meruit

58. Chase Paymentech repeats and re-alleges the foregoing allegations of Paragraphs 1 through 57 as if fully set forth herein.

59. In the alternative to the breach of contract claim above, Chase Paymentech seeks to recover against Landry's under the theory of quantum meruit. Chase Paymentech provided Landry's with payment card processing services that were beneficial for Landry's. In connection with these services, Chase Paymentech was responsible for making the initial payment to the

Payment Brands in the event any assessments, fines, or penalties were issued by the Payment Brands resulting from Landry's failure to comply with the Payment Brand Rules, including the Security Guidelines, or the compromise of any Payment Instrument Information. Landry's bargained for and accepted these services provided by Chase Paymentech.

60. In exchange for these services, Landry's promised to reimburse Chase Paymentech for any assessments, fines, or penalties imposed on Chase Paymentech by the Payment Brands resulting from Landry's failure to comply with the Payment Brand Rules, including the Security Guidelines, or the compromise of any Payment Instrument Information. Landry's was aware that Chase Paymentech expected to be reimbursed for any assessments, fines or penalties by the Payment Brands that Chase Paymentech paid as a result of a credit card data breach as part of the services provided to Landry's.

61. Visa and MasterCard determined that Landry's failed to comply with the Payment Brand Rules, including the Security Guidelines, and that Payment Instrument Information, such as cardholder names, card numbers, expiration dates, and internal verification codes, was compromised in the Data Breach. Indeed, Landry's admitted that Payment Instrument Information was compromised.

62. Following the Data Breach, Chase Paymentech provided Landry's with the GCAR and ADC Assessments issued by the Payment Brands resulting from the Data Breach. The GCAR and ADC Assessments were debited from Chase Paymentech in March 2018. Chase Paymentech requested that Landry's reimburse Chase Paymentech for its payment of the GCAR and ADC Assessments. Landry's failed to pay, and still refuses to pay.

63. Chase Paymentech provided valuable services to Landry's pursuant to the Agreement, and Landry's has a contractual obligation to pay for these services. In the event Chase

Paymentech's breach of contract claim against Landry's should fail, Landry's will be unjustly enriched if Chase Paymentech is not reimbursed for the GCAR and ADC Assessments paid to Visa and MasterCard on behalf of Landry's as a result of the Data Breach.

64. By the conduct alleged above, Landry's accepted services but refused to pay Chase Paymentech for those services, causing Chase Paymentech actual damages. Chase Paymentech is entitled to an award of \$20,062,206.88, in addition to any interest and costs allowed under law.

65. Chase Paymentech also seeks its attorney's fees under Texas Civil Practice & Remedies Code § 38.001(1). This action is founded on services rendered, and Chase Paymentech is therefore entitled to recover its reasonable attorney's fees incurred in addition to the amounts otherwise recoverable.

Count III (In the Alternative) – Promissory Estoppel

66. Chase Paymentech repeats and re-alleges the foregoing allegations of Paragraphs 1 through 65 as if fully set forth herein.

67. In the alternative to the breach of contract claim above, Chase Paymentech seeks to recover against Landry's under the theory of promissory estoppel. Landry's made a promise to Chase Paymentech that Landry's would reimburse Chase Paymentech for any assessments, fines, or penalties imposed by the Payment Brands on Chase Paymentech resulting from Landry's failure to comply with the Payment Brand Rules, including the Security Guidelines, or the compromise of any Payment Instrument Information that led to assessments by the Payment Brands.

68. Visa's GCAR and MasterCard's ADC programs determined that Landry's failed to comply with the Payment Brand Rules, including the Security Guidelines, and that Payment Instrument Information was compromised. Indeed, Landry's has admitted that Payment Instrument Information was compromised as a result of the Data Breach.

69. Chase Paymentech reasonably relied on Landry's promises and paid \$20,062,206.88 to the Payment Brands for the GCAR and ADC Assessments resulting from the Data Breach, as Chase Paymentech was obligated to do pursuant to its contractual obligations to Visa and MasterCard.

70. Chase Paymentech's reliance on Landry's promise to reimburse Chase Paymentech for any assessments, fines, or penalties imposed on Chase Paymentech resulting from Landry's failure to comply with the Payment Brand Rules, including the Security Guidelines, or the compromise of any Payment Instrument Information, was reasonable.

71. As a direct and proximate result of Landry's broken promises, Chase Paymentech has suffered damages in the amount of \$20,062,206.88. Chase Paymentech is entitled to an award of \$20,062,206.88, in addition to any interest and costs allowed under law.

72. Chase Paymentech is also entitled to recover its reasonable and necessary attorney's fees for its promissory estoppel claim. *See Corpus Christi Day Cruise, LLC v. Christus Spohn Health Sys. Corp.*, 398 S.W.3d 303, 314 (Tex. App.—Corpus Christi 2012, pet. denied).

73. If Chase Paymentech's breach of contract claims against Landry's should fail, injustice can only be avoided by enforcing Landry's promise to reimburse Chase Paymentech for any assessments, fines, or penalties imposed on Chase Paymentech resulting from Landry's failure to comply with the Payment Brand Rules, including the Security Guidelines, or the compromise of any Payment Instrument Information.

V. CONDITIONS PRECEDENT

74. All conditions precedent to Chase Paymentech's claims for relief have been performed or have occurred.

VI. TRIAL BY JURY WAIVED

75. The parties have waived trial by jury with respect to this suit. *See* Ex. A, Agreement § 15.10.

VII. PRAYER

76. WHEREFORE, Plaintiffs Chase Paymentech respectfully seek a judgment against Defendant Landry's that includes the following relief:

- a. Actual damages;
- b. Pre-judgment and post-judgment interest;
- c. Court costs;
- d. Attorney's fees; and
- e. All other relief to which Chase Paymentech is entitled.

Dated: May 17, 2018

MORGAN, LEWIS & BOCKIUS LLP

By: /s/ David Levy
David Levy
Attorney-in-Charge
Texas Bar No.: 12264850
S.D. Tex. ID No.: 13725
david.levy@morganlewis.com
Mary Susan Formby
Texas Bar No.: 24083011
S.D. Tex. ID No.: 2292403
marysusan.formby@morganlewis.com
1000 Louisiana Street, Suite 4000
Houston, Texas 77002
(713) 890-5000 Telephone
(713) 890-5001 Facsimile

ATTORNEYS FOR PLAINTIFFS
PAYMENTECH, LLC AND JPMORGAN
CHASE BANK, N.A.